UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/328,726	10/26/98	COLLINS T	2026-25(PT-T

TM21/1226

LEAH SHERRY
OPPENHEIMER, WOLFF & DONNELLY, LLP
1400 PAGE MILL ROAD
PALO ALTO CA 94304

EXAMINER	
LEANING, J	
ART UNIT	**PAPER NUMBER**
2131	14

DATE MAILED: 12/26/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

1- File Copy

Office Action Summary	**Application No.** 09/328,726	**Applicant(s)** COLLINS ET AL.
	Examiner Jeffrey S Leaning	**Art Unit** ~~2766~~ 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

15) ☐ Notice of References Cited (PTO-892)

16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

18) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

19) ☐ Notice of Informal Patent Application (PTO-152)

20) ☐ Other:

DETAILED ACTION

1. Claims 1-13 have been canceled by the applicants. Claims 14-16 are rejected herein.

2. Due to the notation-intensive nature of the application, the examiner will state the conventions that he will use. Underscore marks will denote subscripts, so 'a sub b' will be denoted by 'a_b'. Carets will denote superscripts, so 'a to the b' will be denoted by 'a^b'.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321© may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 14-66 rejected under the judicially created doctrine of double patenting over claims 1-13 of U. S. Patent No. 5,848,159 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Claim 8 of U. S. Patent No. 5,848,159, for example, ` refers to a "succession of invertible operations" which the specification reveals in column 6 lines 1-67 to column 7 lines 1-33 to be the very same operations given by the equations in the claims of the present application.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 14-66 rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura *et al* (US 5,046,094) in view of Menezes *et al*.

a. Claim 14 is directed to a method for establishing cryptographic communications. Kawamura teaches of a computation method for processing secret information, see the abstract.

i. Both Kawamura *et al* and the applicants use RSA-type cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Kawamura *et al*, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants and Menezes *et al*, there are possibly more than two prime numbers in the modulus and they are called p_1, p_2, ... , p_n. Hence, p corresponds to p_1, and q corresponds to p_2. This is merely notation, and the examiner point it out for the sake of clarity.

ii. Kawamura *et al* teach of encoding a plaintext word M to a ciphertext word C where M is less than or equal to n-1 where n is the product of two primes, see column 1 line 46.

iii. Kawamura *et al* teach of transforming ciphertext C to message M, see the abstract.

iv. Kawamura *et al* teach of calculating the quantities of claim 14, see equations (18), (19), (24) and (25) in columns 8-10 of Kawamura *et al*. The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' e_1 corresponds to Kawamura *et al*'s r_p. The applicants' e_2 corresponds to Kawamura *et al*'s r_q. The applicants' C_1 corresponds to Kawamura *et al*'s X_p. The other correspondences are analogous.

v. The number 'e' is selected as being relatively prime to the described lcm (least common multiple), see column 1 lines 24-50.

vi. Kawamura *et al* calculate the other quantities of claim 14, see the numbered equations of Kawamura *et al*: (21)-(32) in columns 9-12, especially (37). The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' w_2 corresponds to Kawamura *et al*'s p. The applicants' (w_2^-1 mod p_2)mod p_1]p_1 mod n corresponds to Kawamura *et al*'s w_q=p(p^-1 mod q) mod n. And of course, the applicants' M corresponds to Kawamura *et al*'s M and the applicants' C corresponds to Kawamura *et al*'s C.

vii. Kawamura *et al* lack a teaching that there can be more than two primes in the modulus and that the message M is transformed to ciphertext C using the steps described in paragraphs 6.a.iii-vi above.

(1) The examiner takes official notice that encryption and decryption are inverse operations. It would be obvious to one of ordinary skill in the art to use the above steps for encryption because inverse operations are performed using the steps in an inverse manner.

(2) Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes p_1^e1 p_2^e2 ... p_k^ek, see definition 3.3. It would be obvious for one of ordinary skill in the art to modify the system of Kawamura *et al* to have a modulus having the number of primes, 'k', being a number greater than 2.

b. Claim 15 is similar to claim 14 except the message is decrypted using the corresponding formulae and steps. See the above.

c. Claim 16 is directed to a cryptographic communications system. Kawamura *et al* teach of a distributed secret information processing unit, corresponding to the applicants' cryptographic communications system, see the abstract.

i. Both Kawamura *et al* and the applicants use RSA-type cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Kawamura *et al*, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants and Menezes *et al*, there are possibly more than two prime numbers in the modulus and they are called p_1, p_2, ... , p_n. Hence, p corresponds to p_1, and q corresponds to p_2. This is merely notation, and the examiner point it out for the sake of clarity.

ii. Kawamura *et al* teach of an encrypting means and a communication medium, see the abstract.

iii. Kawamura *et al* teach of enciphering a message in the manner of the applicants, using the formulas of the claim, see column 1 line 46.

iv. The number 'e' is selected as being relatively prime to the described lcm (least common multiple), see column 1 lines 24-34.

v. Kawamura *et al* teach of a decoding means for receiving C and transforming C, see the abstract.

vi. Kawamura *et al* calculate the last two quantities of claim 16 (lines 21-23), see the numbered equations of Kawamura *et al*: (21)-(32) in columns 9-12. The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to

Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' w_2 corresponds to Kawamura *et al*'s p. The applicants' Y_1 corresponds to Kawamura *et al*'s C. The applicants' (w_2^-1 mod p_2)mod p_1]p_1 mod n corresponds to Kawamura *et al*'s w_q=p(p^-1 mod q) mod n. And of course, the applicants' M corresponds to Kawamura *et al*'s M and the applicants' C corresponds to Kawamura *et al*'s C.

vii. Kawamura *et al* lack a teaching that there can be more than two primes in the modulus. Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes p_1^e1 p_2^e2 ... p_k^ek, see definition 3.3. It would be obvious for one of ordinary skill in the art to modify the system of Kawamura *et al* to have a modulus having the number of primes, 'k', being a number greater than 2.

d. Claims 17-21 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

e. Claims 22-26 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

f. Claims 27-31 are method claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

g. Claims 32-36 are system claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

h. Claims 37-41 are method claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 15.

i. Claims 42-46 are system claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 16.

j. The examiner takes as official notice that it is notoriously well-known to those of ordinary skill in the art to use RSA type cryptography for signing and verifying messages. It would be obvious to one of ordinary skill in the art to use RSA type cryptography to sign messages and verify such signatures because of the security and irrefutability available from such expedients.

i. Claims 47-51 are method claims for signing a message and are rejected on grounds analogous to those used to reject claims 14 and 15 and further in light of the above official notice.

ii. Claims 52-56 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

iii. Claims 57-61 are procedure claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

iv. Claims 62-66 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

Response to Arguments

7. Applicant's arguments filed 17 October 2000 have been fully considered but they are not persuasive.

a. The applicant has traversed the double patenting rejection of claims 14-16. The applicant states that the examiner used an impermissible interpretation of the phrase "succession of invertible operations." The examiner responds by noting that even though the phrase "succession of invertible operations" may not appear in the columns 6 and 7 of the specification, a description of a succession of invertible operations does. The applicant argues that the phrase refers to operations appearing in parent claim 7. The examiner notes that there is no evidence, such as a reference to an antecedent in claim 8, to support this assertion. The examiner maintains his double patenting rejection.

b. The applicant argues that Menezes *et al* does not disclose that an RSA modulus may consist of a product of more than two primes.

i. The applicant misconstrues part of the examiner's argument as follows. The applicant, relying on a mathematical notational tradition of denoting an RSA modulus as the particular letter "n", presumes that the sequence of primes disclosed by Menezes *et al* “p_1,p_2,...,p_n”, when multiplied together, produce n. The examiner points out the fault in this assumption by noting that the subscript in Menezes *et al* and in the action is “n”, not the modulus, in the context of the present argument. *The applicant, in fact, misquotes the examiner* on page 30 of the amendment by erroneously inserting an “n” into item 6.a.i. of the examiner’s rejection, and this may help explain the dispute.

ii. The applicant further states that Menezes *et al* “merely recites” a “fundamental theorem.” For the sake of clarity, the examiner points out that the passage in question in Menezes *et al* is a definition, and not a theorem. The examiner points out that theorems require proof. Menezes *et al* item 3.3 is labeled “Definition” and lacks a proof. It is not the fundamental theorem of arithmetic for which the applicant mistakes it.

iii. The examiner reaffirms his argument by restating the evidence that Menezes *et al* suggests an RSA modulus of more than two primes in the form of a simple syllogism. Major Premise: the RSA algorithm derives its security from the difficulty of the integer factorization problem as applied to the modulus (well-known to one of ordinary skill in the art). Minor premise: the integer factorization problem consists of factoring numbers of the form p_1^e1 * p_2^e2 * ... * p_k^ek (explicit in Menezes *et al* definition 3.3). Conclusion: Menezes *et al* definition 3.3 provides motivation for using an RSA modulus of the form p_1^e1 * p_2^e2 * ... * p_k^ek. That is, this definition provides motivation for using a product of more than two primes as an RSA modulus.

c. The applicant further argues that the Chinese Remainder Theorem (hereinafter "CRT") does not provide for solving (1) k simultaneous equations or (2) the necessity of combining the results in an efficient manner. To the contrary, the CRT, which has been known for centuries, is a mathematical tool for doing exactly those two steps. That is, the CRT has been used for centuries for solving systems of modular equations by solving sub-equations and combining them together to get a solution in an efficient manner. The examiner asserts that one of ordinary skill in the art is aware that the CRT accomplishes this purpose. Further, both Menezes *et al* and Kawamura *et al* disclose using the CRT in the context of solving the multiple modular equations which arise when dealing with mathematical aspects of using RSA. That is, both references provide *explicit usage of the Chinese Remainder Theorem in RSA cryptography.* Hence, motivation to combine is provided, in the sense that *the combination of CRT with RSA already exists in both references.*

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Quisquater *et al* teaches of using the Chinese Remainder Theorem (as the applicants do to derive the formulas in the claims) in association with RSA cryptography and cites many benefits, see formula (1) on pp. 906 in particular. Naciri (US 5,761,310) also teaches of using formulas corresponding to the applicants' in the same setting, see figure 3 for example.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Scott Leaning whose telephone number is (703) 306-5975. The examiner can normally be reached on weekdays from 9:00am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned is (703) 308-9051.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jeffrey Scott Leaning

19 April 2000

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100